

AMENDMENTS TO THE SPECIFICATION

Please replace Paragraph [0052.2] with the following paragraph rewritten in amendment format:

[0052.2] The embodiment of the present invention also provides a method for a digital certificate issuing system with intrusion tolerance ability issuing digital certificate, the method includes:

~~splitting a private key into multiple first sub-secret-keys and multiple second sub-secret-keys, wherein the private key is constructed by one second sub-secret-key and t first sub-secret-keys, the second sub-secret-key corresponds to the t first sub-secret-keys according to an equation combination representation, and the number t is a positive integer~~ splitting a private key into multiple first sub-secret-keys and multiple second sub-secret-keys, wherein the multiple first sub-secret-keys are divided into k groups, and the private key is constructed by one second sub-secret-key and t first sub-secret-keys, the second sub-secret-key corresponds to the t first sub-secret-keys according to an equation combination representation including t items of j and i, j is sequence number of the group which has the first sub-secret-key, and i is number of the first sub-secret-key in the jth group, each of j in one equation combination representation is different, j, i, k, and t are positive integers, and t is less than k;

calculating t first calculation results according to ~~the a~~ a certificate to be signed and the t first sub-secret-keys in the multiple first sub-secret-keys upon receiving ~~a the~~ a certificate to be signed;

obtaining the second sub-secret-key corresponding to the t first sub-secret-keys according to the equation combination representation;

calculating a second calculation result according to the second sub-secret-key obtained and the certificate to be signed;

generating a digital signature according to the t first calculation results and the second calculation result;

generating a digital certificate according to the digital signature and contents of the certificate to be signed.